Amendments to the Specification:

Please replace the paragraph beginning on page 8, line 6 with the following amended paragraph:

FIG. 1 depicts a typical flow for a cryptographic application. In step 102, preparatory calculations are performed. These calculations are done once for an entire set of data that requires encryption. In step 102, the encrypting transform is generated, wherein the choice is made as to the form of the encrypting transform and the mathematical equation to represent the encrypting transform. For instance, the choice is made to use a certain mathematical curve type such as a polynomial curve, an elliptical curve, or a cyclotomic polynomial curve as the encrypting transform. It is understood from these examples that the form of the encrypting transform is fundamentally algebraic. After this choice is completed, an equation is determined by choosing coefficients for the mathematical equation representing the encrypting transform. Examples of choosing coefficients for equations for elliptical curve types are found in *Implementing Elliptical Curve Cryptography* by Michael Rosing (Manning Publications, 1999) on pages 133-136. Other parameters may be chosen in this step, such as with elliptical curves, a base point is typically chosen, as described by Rosing on pages 174-188.

Please replace the paragraph beginning on page 16, line 8 with the following amended paragraph:

When color digital images are the data to be encrypted and decrypted, other embodiments are evident. Digital images are arrays of small entities called pixels. Each pixel represents a portion of the image scene. Such digital images are also known in the art as raw digital images. When the digital images are color digital images, each pixel, typically, has three values representing the three components, red, green, and blue, which together represent the color of that portion of the scene. The three red, green, and blue values together comprise a point in a three dimensional color space defined by an industry standard. There are many such standards. Typically, for any given image, the user understands the industry standard and the three dimensional color space in which the red, green, and blue values are defined. Examples of these color spaces and industry standards can be found in any color science textbook. A noteworthy one is *A Technical Introduction to Digital Video*, by Charles Poynton (Wiley & Sons, 1996).

Please replace the paragraph beginning on page 18, line 20 and ending on page 19, line 14 with the following amended paragraph:

In this invention, a pixel's red, green, and blue values are converted to its respective CIE XYZ values after which the respective fundamental metamer, a component black metamer, and a component radiometric function are calculated. The metamers and radiometric function are preferably stored in the computer memory as floating point binary numbers. Preferably, 31 points are used to represent the visible spectrum, so there will be 31 floating point numbers for each of the metamers and the radiometric function. Any one or any combination of the floating point numbers of the metamers and the radiometric function, referred to as the radiometric expression, is used in the cryptographic system. The floating point numbers in binary can be concatenated together to form a large precision integer. It will be recognized that the floating point numbers can be concatenated to form sequences of any length. In one embodiment, a floating point or high precision integer from the radiometric expression would be used as the x value in the calculation of the base point in Step 102 of FIG. 1. This allows the base point is be calculated for each block of data in Step 106, rather than once for the entire set of data in Step 102. A more secure cryptographic system results. If a third party intercepts and pirates a base point, they have access to only one block of data rather than the entire set of data. In addition, the metamers and radiometric function are calculated from the data itself allowing no extra information to transmit from the sender to the receiver for the data to be decrypted. Again, a more secure cryptographic system results.